REMARKS/ARGUMENTS

This communication is in response to the Advisory Action dated October 27, 2009 and Final Office Action dated August 18, 2009. Claims 1-14 were previously canceled, without prejudice. New independent claim 32 has been added. No new matter has been added. Claims 15-32 remain pending in this application with claims 15, 26 and 32 being the only independent claims. Reconsideration is respectfully requested.

Prior Art Claim Rejections

Claims 15, 18, 21-23, 25 and 27 are rejected under 35 U.S.C. §103(a) as obvious over US Patent Publication No. 2003/0107648 (Stewart et al.) in view of US Patent Publication No. 2003/0112354 (Ortiz et al.).

Claims 16, 17, 19, 20 and 24 are rejected under 35 U.S.C. §103(a) as obvious over Stewart et al. and Ortiz et al. in view of US Patent No. 6,930,994 (Stubbs).

Claims 26 and 29-31 are rejected under 35 U.S.C. §103(a) as obvious over Ortiz et al. in view of US Patent Publication No. 2003/0020611 (Script et al.).

Claim 28 is rejected under 35 U.S.C. §103(a) as obvious over Ortiz et al. in view of Script et al. and Stubbs.

Applicant respectfully traverses the prior art rejections for at least the reasons discussed below.

Independent Claims 15 & 26

Claim 15 calls for "checking that a subscriber relationship (8, 9) of the mobile communication system and/or a temporary IP address is associated with a corresponding transmitter and receiver, wherein the two subscriber relationships and/or the IP addresses are linked in a database of the operator (11) of the mobile communication system." (emphasis added)

The Examiner acknowledges that Stewart et al. fails to disclose or teach these claimed limitations, stating instead that they are taught by Ortiz et al. (paragraphs [0071], [0073], [0076]). Referring to the relevant paragraphs cited by the Examiner, Ortiz et al. discloses "Additionally, a security unit may be utilized to process proper security codes to thereby ensure that data

transferred to and from hand held device 11 may be secure and/or permitted. Broadcast security prevents general receipt of venue images without proprietary hardware and/or signals." (paragraph [0058]) Ortiz et al. further states that "The equipment may also provide for the securing transmission of signals and associated data. For example, such equipment can rely on the encryption of signals. These signals, if encrypted, can be decrypted by authorized hand held receivers." [0071] Accordingly, Ortiz et al. teaches that only authorized hand held receivers employ the necessary hardware/software to decrypt the encrypted data. The reference fails to disclose or suggest a database for linking the two subscriber relationships and/or the IP addresses, as expressly called for in claim 15.

Addressing now the Examiner's remarks in the October 27, 2009Advisory Action. Initially the Examiner discusses the "and/or" limitation found in claim 15. This "and/or" limitation is to be interpreted in accordance with well establish patent law as requiring one limitation, the other limitation or both. Thus, in the present claimed invention, claim 15 requires the linking between a transmitter and a receiver of the following: (i) "subscriber relationships"; (ii) "IP addresses"; or (iii) both subscriber relationships and IP addresses. Applicant asserts that Ortiz et al. fails to disclose or suggest any of these three conditions. The Examiner acknowledges in the Advisory Action that Ortiz et al. discloses "the handheld device having cartridge/module wherein [sic] contain security code, encryption/decryption codes that allow the handheld device authorized to access retrieve real time video image, (paragraph [071], [0073]), further clarify in paragraph [0058-0059] that security unit checking or process proper security code to ensure that data transfer to and from handheld device is permitted." {October 27, 2009 Advisory Action: p. 2, ll. 14-16}

The security codes and encryption/decryption codes are merely hardware/software included in the handheld device that if present permits the signal to be decrypted. There is no linking of data (e.g., subscription information, IP addresses or both) between transmitter and receiver in a database, as found in claim 15.

In the August 18, 2009 Final Office Action the Examiner stated that Ortiz et al. reads on the first condition "when handheld device authorized than the handheld device received video and decrypted which is read on checking subscriber relationship authorization for receiving video data." {August 18, 2009 Final Office Action: p. 2, last sentence through p. 3, l. 2} Applicants

respectfully disagree. Such authorization as taught by Ortiz et al. is conditional merely on the presence of decryption hardware/software that is either installed or accessible by the receiver without any linking of the two subscriber relationships themselves.

Claim 15 further includes the step of "checking authorization of the receiver for receiving the video data from the transmitter, based on the linked data." No such checking or verification as to proper authorization of the receiver based on the linking of the two subscriber relationships (since the Examiner acknowledges that Ortiz et al. fails to disclose linking of the IP addresses) is disclosed by the reference. Instead the only condition for authorization is whether the proper decryption software is provided on or accessible by the receiver, then authorization is assumed to be valid. No authorization for the receiver to receive the transmission is conditional on the linking of the two subscriber relationships.

Claim 26 is the apparatus counterpart of method claim 15. Despite the fact that claims 15 and 26 are counterparts of one another, the Examiner maintains the prior art rejection of claim 26 on different grounds than that used to reject claim 15. It is also noted, that the Examiner with respect to claim 26 acknowledges that Ortiz et al. fails to disclose "a database of the mobile communication system for linking two subscriber relationships and/or addresses" and "a device (10) for checking, based on the data stored in the database, if a subscriber relationship (8, 9) of the mobile communication system and/or IP address associated with the transmitter and the receiver are linked; and if the receiver is authorized to receive the video data from the transmitter." {August 18, 2009 Final Office Action: p. 8, 17 through p. 9, l. 2} These limitations are merely the apparatus counterpart of the last two steps in method claim 15 which the Examiner maintains are taught by Ortiz et al. Therefore, there is inconsistency in the Examiner's arguments with respect to claims 15 and 26.

The Examiner's rejection with respect to claim 26 will now be addressed. In the outstanding Office Action the Examiner acknowledges that certain limitations in claim 26 are not disclosed by Ortiz et al. and yet maintains such limitations are nevertheless taught by Script et al. First, Applicants assert that the two references are clearly non-analogous prior art references. MPEP §2141.01(a)(I) provides "Thus a reference in a field different from that of applicant's endeavor may be reasonably pertinent if it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his or her

invention as a whole." Applying these principles to the present situation the two references are in different fields. Ortiz et al. is directed to wireless transmission of in-play camera view to hand held devices while Script et al. relates to a portable motion detector and security alarm method and system. Such different fields of invention would not have logically commended themselves to being drawn to the attention of one of ordinary skill in the art.

Even assuming, *arguendo*, that the two references are analogous prior art, the combination fails to teach the present claimed invention. Script et al. fails to disclose "a database of the mobile communication system for linking two subscriber relationships and/or IP addresses." The relevant passage from Script et al. reads "There is also connected to the computer host 261 a large capacity data storage resource 264 (such as a storage array, a storage network, etc.) that stores a subscription database containing subscriber information for multiple subscribers. The subscription information includes data sets that correlate the unique identifiers associated with each subscriber's motion sensing and transmitting means 20 with *object identification information specified by the subscriber*." (paragraph [0107]) Thus, in contrast to the present claimed invention calling for a database "linking two subscriber relationships", Script et al. discloses subscription information correlating for each subscriber unique identifiers associated that that subscriber's motion sensing and transmitting means with object identification information specified by that same subscriber, the relationships among two subscribers are not correlated.

Since no two subscriber relationships are correlated, Script et al. also fails to disclose or suggest "a device (10) for checking, based on the data stored in the database, if a subscriber relationship (8, 9) of the mobile communication system and/or IP address associated with the transmitter and the receiver are linked; and if the receiver is authorized to receive the video data from the transmitter."

Dependent Claims 17 & 28

Claim 17 specifies "setting up a connection between transmitter and receiver by dialing the associated mobile subscriber telephone number (MSISDN) or an IP address." In rejecting claim 17 the Examiner states that Stewart et al. (Col. 6, ll. 15-20) reads on this limitation. The passage referred to by the Examiner states "The PUD [Packet User Database] 52 holds call group

records for identifying the members of a call group. Referring to FIG. 4, which shows an exemplary call group record, a field for a single call group is identified by a call group ID containing fields 60, two or more mobile station IDs, MSID1, MSID2,...,MSIDn are contained in fields 62, and each mobile station ID field 62 has an associated call seize field 64 flagged to indicate that the associated mobile station has currently seized the call group." (emphasis added) Stewart et al. discloses mobile station IDs (e.g., MSID1, MSID2,...,MSIDn), not telephone numbers dialed to set up a connection between transmitter and receiver, as found in claim 17.

Claim 28 is a similar apparatus counterpart of method claim 17. Despite the fact that claims 17 and 28 are counterparts of one another, the Examiner rejects claim 28 on different grounds using different prior art than that used to reject claim 17. It is the Examiner's position that the limitation in claims 17 and 28 is taught by Stubbs. The passage in question (Col. 1, ll. 55-65) merely discloses storing international mobile subscriber identification (IMSI) in a home location register (HLR), but fails to disclose storing associated mobile subscriber telephone number (MSISDN) for setting up the call by dialing the telephone number.

In the October 27, 2009 Advisory Action the Examiner clarified his position by stating "Stubbs teaches setting up virtual connections between GPRS users (mobile station) and the PLMN and in order to carried [sic] out the connection, the user initiate from the mobile station. Since the prior art does not mention 'dialing the associated mobile subscriber telephone number', it would lead one skill [sic] to take account 'user initiate from the mobile station' which dialing the mobile station." {October 27, 2009 Advisory Action: p. 2, ll. 25-28}

Applicant respectfully disagrees and draws the Examiner's attention to Stubbs which expressly states "The GGSN provides a mapping function for mapping a packet data protocol (PDP) address, whereby a mobile user is identified to the packet data network 46, to a mobile station identity, whereby the mobile user is identified in the PLMN. The PDP address of a mobile user conforms with the standard addressing scheme of the respective network layer service used in the packet data network 46, for example an IP version 4 address, an IP version 6 address or an X.121 address." (Col. 4, l. 67 through Col. 5 l. 9) Thus, the connection is established via a PDP address, not by dialing of an MSISDN.

Dependent Claims 18 & 29

Claim 18 provides "storing routing rules for transmitting video data between the transmitter and receiver in the database." (emphasis added) It is the Examiner's position that this limitation is taught by paragraphs [0018]-[0019] of Stewart et al. Applicant respectfully disagrees. Stewart et al. discloses that "The hub 16 includes a router 28 that routes video streams to requesting clients 14 using a wireless link. The clients 14 can access the video streams by establishing communication with the hub 16 and authenticating themselves to a conditional access module 30 at the hub 16. That is, to access a particular stream a client 14 establishes communication with the hub 16 and requests a particular video stream from a client-selected location 12, with the conditional access module 30 permitting (or not) the client 14 to receive the selected stream, depending on the client's authentication. Consequently, access to the surveillance video streams generated by the sources 18 can be controlled by the hub 16 on a client-by-client basis." (paragraph [0019])(emphasis added) Thus, transmission is dependent exclusively on authentication by the client irrespective of from where the video originated (transmitter), rather than routing rules between the transmitter and receiver, as called for in claim 18.

The Examiner in the October 27, 2009 Advisory Action in maintaining the rejection states "Stewart clearly teach [sic] the transmitter 24 sending video to the system hub 16 wherein the hub 16 routes video stream to the clients using wireless link which read on routing transmitting video data between the transmitter and receiver in the database...." {October 27, 2009 Advisory Action: p. 2, ll. 35-37} The mere fact that Stewart discloses a hardware router 28 for routing video streams to requesting clients, the prior art reference fails to disclose or suggest such transmission being based on "routing rules" stored in a database, as found in claims 18 and 29.

Claim 29 is the apparatus counterpart of method claim 18. Despite being the apparatus counterpart of method claim 18, claim 29 is rejected on different grounds. Addressing the prior art rejection with respect to claim 29 being taught by Ortiz in paragraph [0082]. The paragraph in question reads "Those skilled in the art can appreciate that although real time video data may be transmitted to server 100, captured past video images may also be stored within server 100 and transferred to hand held device 60 for display at display screen 61. For example, instant

replays may be transferred as video data to hand held device 60 upon the request of a user of hand held device 60. Such instant replay footage can be displayed on display screen 61 for the user to view." (emphasis added) Ortiz et al. fails to disclose or suggest routing rules for transmitting video data between the transmitter and receiver being stored in the database. Instead, sever 100 stores captured video images and transfers them at the request of a user of hand held device 60. No mention is made of transmission being based on routing rules or of the server 100 storing such information.

Dependent Claim 22

Claim 22 states "setting up a connection or transmitting data between transmitter and receiver only based on a triggering event." (emphasis added) In rejecting the claim the Examiner maintains that this limitation is taught by Stewart et al. in Figure 1 and the disclosure associated therewith. Applicant respectfully disagrees. Stewart et al. teaches transmission of data only after receiving a request from the client 14 (paragraphs [0017], [0019]), rather than based on a "triggering event."

In the Advisory Action the Examiner appears to acknowledge that Stewart et al. fails to disclose or suggest the claimed limitation, but nevertheless concludes that "Stewart clearly teach [sic] the method of surveillance that generating video of a surveillance location using camera and when the motion is detected, video can be generate and send to mobile wireless receivers. That is, this read [sic] on 'setting up a connection or transmitting data between transmitter and receiver based on a triggering event' (Paragraph [0006] and Fig. 1 Illustrate and described)" {October 27, 2009 Advisory Action: p. 2, ll. 46-49}(emphasis added)

Addressing the Examiner's remarks, claim 22 calls for "setting up a connection or transmitting data between transmitter and receiver only based on a triggering event." (emphasis added) The Examiner asserts that the triggering event is the detection of motion. Stewart et al. fails to disclose or suggest that a connection is established and data is transmitted upon motion being detected. Stewart et al. teaches transmission of data only after a request from the client 14 (paragraphs [0017], [0019]) is received rather than a "triggering event," much less, the specific triggering event of detection of movement by a motion sensor or a regularly scheduled time interval. Stewart et al. does disclose a motion sensor 39 as an indication of motion in a location 12 but only for the purpose of establishing the frame rate not to trigger setting up a connection or transmitting

data. Data is transmitted regardless of whether any motion is detected, only the frame rate of transmission varies depending on the detected motion at a location.

Nevertheless, the Examiner rejects the claim by concluding that a connection and transmission of data can be triggered based on the detection of motion. Applicant respectfully disagrees because the claim calls for connection and transmission only upon the triggering event (which the Examiner asserts is analogous to the detection of motion). Instead, Stewart et al. discloses setting up a connection or transmitting data other than upon the detection of motion (e.g., upon the client making a request) and thus does not read on the present claimed invention. Even assuming, *arguendo*, that Stewart et al. could be modified to establish a connection and transmit data upon detecting motion it also performs these functions upon receiving a request from a client and thus fails to read on the present claimed invention.

Dependent Claim 27

Claim 27 depends from claim 22 and further specifies "wherein the triggering event is detection of movement by a motion sensor or a regularly scheduled time interval." As discussed above with respect to claim 22, from which claim 27 depends, Stewart et al. teaches transmission of data only after a request from the client 14 (paragraphs [0017], [0019]) is received rather than a "triggering event," much less, the specific triggering event of detection of movement by a motion sensor or a regularly scheduled time interval. Stewart et al. does disclose a motion sensor 39 as an indication of motion in a location 12 but only for the purpose of establishing the frame rate not to trigger setting up a connection or transmitting data. Data is transmitted regardless of whether any motion is detected, only the frame rate of transmission varies depending on the detected motion at a location.

In the outstanding Office Action the Examiner rejects claim 27 as being taught by paragraph [0056] of Ortiz et al. The claim expressly calls for the specific type of sensor as being "detection of movement by a motion sensor." Ortiz et al. fails to explicitly mention a sensor. Paragraph [0056] of Ortiz et al. to which the Examiner refers discloses a sound generator and speaker. Thus, Stewart et al. and Ortiz et al. either alone or in combination thereof clearly do not establish a connection and transmission only upon detecting movement by a motion sensor or regularly scheduled time interval.

Independent Claim 32

Claim 32 specifies "stored data includes an international mobile subscriber identification (IMSI), a mobile subscriber telephone number (MSISDN) and a temporary IP address." (emphasis added) New independent claim 32 differs from independent claims 15 and 26 in that the stored data includes all three pieces of information namely, IMSI, MSISDN and temporary IP address. For at least the reasons discussed above with respect to claims 15 and 26, the prior art of record fails to disclose or suggest that the stored data in the database linking the transmitter and receiver includes all three of the claimed pieces of information.

For at least the foregoing reasons, Applicant submits that claims 15-32 are patentable over the prior art of record and passage of this application to issuance is therefore requested.

CONDITIONAL PETITION FOR EXTENSION OF TIME

If entry and consideration of the amendments above requires an extension of time, Applicants respectfully request that this be considered a petition therefor. The Assistant Commissioner is authorized to charge any fee(s) due in this connection to Deposit Account No. 14-1263.

ADDITIONAL FEE

Please charge any insufficiency of fees, or credit any excess, to Deposit Account No. 14-1263.

Respectfully submitted,

NORRIS McLAUGHLIN & MARCUS, P.A.

By /Christa Hildebrand/

Christa Hildebrand
Reg. No. 34,953
875 Third Avenue - 8th Floor
New York, New York 10022
Phone: (212) 808-0700
Fax: (212) 808-0844
Facsimile: (212)808-0844

001418510CH/CFC